Statement
Colonel Randall J. Larsen, USAF (Ret)
Founder and CEO Homeland Security Associates, LLC
Before the Committee on the Budget
United States House of Representatives
National and Homeland Security: Meeting the Needs
February 16, 2005

Introduction

Mr. Chairman and distinguished members, I began my study of homeland security in 1994, and in January 1995 published my first monograph on the subject. Since then I have been actively engaged in the study of securing the American homeland. In 1998, while serving as the Chairman, Department of Military Strategy and Operations at the National War College, I created the nation's first graduate course in homeland security, and in 2000 I founded the ANSER Institute of Homeland Security. After more than a decade of research, writing, teaching and consulting in both the public and private sectors, I must admit that I still have much to learn about this dynamic and complex subject.

Nevertheless, I am pleased to have the opportunity today to offer my analysis and recommendations for homeland security spending priorities. For the past several months, this has been the focus of my research efforts and the main theme of my forth coming book, *Our Own Worst Enemy: The Terrorist Threat is Real, but our Responses to 9-11 May Pose a Greater Threat.*

Mr. Chairman, and distinguished members, if we, as a nation, do not develop a comprehensive strategy and supporting fiscal priorities for defending our homeland, then our own incompetence will become a greater threat to our security than al Qaeda. If we do not display the wisdom, vision and courage to properly analyze the new security environment; develop a long-range, comprehensive strategy; and provide bi-partisan priorities for the tough budgetary decisions that lay ahead, then I have serious concerns about the security of our nation.

When the Cold War ended General Colin Powell predicted it would take a decade before we understood the new international security environment. We all knew it was transforming from bi-polar to multi-polar or perhaps, uni-polar, but our intelligence community, executive and legislative branches of government, and the academic community failed to understand the role that technology would play in shaping the new security era--what we now call homeland security.

Fifty years ago, Osama bin Ladin would have just been another angry guy in the desert with an AK-47. In the 21st century, technology provides bin Ladin, and those who will follow, with the means to threaten a superpower. In the decade preceding 9-11, we failed to recognize this.

We must not fail a second time. Or, to borrow a phrase from President Harry Truman, "No learning takes place the second time you are kicked by a mule."

To provide a better perspective for my comments, let us assume for a moment that it has not been three and one half years since the last attack on our homeland. Let us assume that a large-scale attack occurred just a week ago. I ask you, "In light of the most recent attack, what are your spending priorities?" You might respond, "What type of attack just occurred?" And I would say, "That is totally irrelevant."

We, not the enemy, must be in charge of our destiny. The priorities I give you today will remain constant over the next decade, regardless of what is in the next news cycle. This is true because I am giving you strategic advice, not tactical. We have spent far too much time thinking about homeland security from the tactical rather than from the strategic level, and this is not the first time that America's national security leaders have had difficulty with the strategic perspective.

When General Eisenhower returned from World War II, he stated that American military officers were equal to the British officers at the tactical and operational levels. However, when it came to the strategic thinking, the British officers were far superior. Ike said, "Fix it." And that Mr. Chairman is why the National War College was created--to teach our future military leaders to think strategically. It has produced many strategic thinkers, including General Brent Scowcroft and Secretary of State Collin Powell. That is what is sorely missing in the homeland security community today--strategic thinking. So that is where I will begin.

Strategy First

I understand you asked me here today to provide my recommendations for spending priorities. I understand that priorities are the bottom-line of this hearing and this committee, but if I immediately go to them, then I would be guilty of committing one of the most common mistakes made in Washington DC: "ready, shoot, aim." I have seen this repeatedly during the past decade. We began spending money on homeland security in 1996. After 9-11, we vastly increased the rate of spending, but it was not until the summer of 2002 that we actually published a national strategy for securing the homeland. And even then, it was not really a strategy. The principal author of the document agrees it is not a strategy; he said it is a "good plan."

Mr. Chairman, we still do not have a long-range, comprehensive strategy for defending the American homeland. Without one, how can I possibly recommend spending priorities? If we do not know where we are headed, how can I offer a plan to get us there? Therefore, I submit as an attachment to this statement, my statement from a hearing on February 3, 2004 before the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations. (Attached)

In that hearing I was asked to provide an analysis of the Administration's strategy for defending our homeland. I examined eight strategies that had been released by the

Administration since 9-11, and found them to be primarily plans focused on subjects ranging from cyber security to money laundering and counter terrorism. None, however, provided a long-range, comprehensive strategy--a strategy that would stand the test of time as did George Kennan's *containment*. Containment was the strategy that guided eight presidents and twenty congresses and eventually led to victory in the Cold War. That is the type of strategy that is needed today.

I will not repeat my entire testimony from last February, but let me say that I did not end my statement with just a critical analysis of the Administration's efforts--I also offered my recommendation for a strategy. Despite the fact that I still do not particularly like the name I gave this strategy, I have yet to find a better one. I called it *containment*. But containment, Mr. Chairman, in the 21st century is far different than the containment George Kennan spoke of nearly six decades ago.

Excerpt from the February 3, 2004 statement:

> It is unrealistic and even naïve to believe that we can permanently end terrorism or terrorist threats to our homeland. One of the candidates for President recently stated in a television advertisement that he could prevent attacks on the American homeland--a preposterous idea that he quickly withdrew. Nevertheless, in the case of defending our homeland, we all hate to admit that which is true. We cannot defeat terrorism.
>
> We cannot win the War on Terrorism as we did the war on fascism. Unconditional surrender by the Germans and Japanese ended the threat. That is not possible today. Secretary Ridge has stated there will be no victory parades. He is absolutely correct. Therefore, let us make our strategy reflect this reality. We should seek to control certain factors, or better yet, *contain* the threat from terrorism.
>
> We must *contain* the capabilities, global reach, and financial resources of terrorists and terrorist organizations. We must *contain* the proliferation of weapons of mass destruction, particularly those weapons that most threaten our survival, nuclear and biological. We must *contain* the spread of hatred with our own offensive campaign in the war of ideas. We must *contain* the vulnerabilities of our nation. And we must seek to *contain* our response to the new threats. We must not overreact.
>
> Some will comment that this is a defeatist strategy. I say it is realistic. We cannot stop every determined truck bomber, but we must prevent a mushroom cloud over an American city or a catastrophic biological attack on the nation. We can't kill, capture, or deter every terrorist, but must *contain* them by limiting their capabilities, their global reach and financial resources.

We cannot prevent the proliferation of all weapons of mass destruction. Chemical agents, including industrial chemicals are far too easy to produce or buy. Radiological material for use in a dirty bomb has already proliferated beyond control. It exists in most hospitals, laboratories, and even at many large construction sites around the world. However, we must *contain* the proliferation of nuclear weapons and biological weapons. Programs such as Nunn-Lugar are great investments in homeland security.

The Wahabi sect of Islam supports schools, organizations, and special programs, some in our own country. Registered with the IRS as 501 (c) 3 charitable institutions they preach hatred and violence against America and Americans. We cannot end all coordinated information campaigns against the United States, but we must retaliate with our own offensive campaign to *contain* this contagion of hatred, disinformation, and instigation.

We are a free and open nation. That makes us a target-rich environment for terrorists. We must take prudent and fiscally responsible actions to reduce these vulnerabilities and implement realistic and measurable prevention and incident management programs. The measurement part is critically important. If we do not set standards and goals, how can we measure progress?

One distinguished group of Americans released an often quoted report last year calling for an *increase* in spending on security within US borders that would approach $100 billion over five years. But we have yet to establish standards and measurable goals for such programs. How did they determine these numbers? How would Congress allocate and prioritize spending? It would be a great for pork. It would send money to every Congressional district. But would it make us more secure?

The press has a field day when a college student smuggled a few box cutters on an airliner, but do we really want a security system that is 100 percent successful? If so, it will take us hours to get through an airport. A system that is 80 percent effective is not an attractive target--even to a suicide bomber. A system that stops four out of five attackers is a strong deterrent, and one we can afford. If it is part of a layered defense, it will provide the security required. A passenger and cargo screening system, backed up by hardened cockpit doors, thousands of armed sky marshals, armed pilots, and passengers who have not forgotten Todd Beamer and his compatriots is the type of security system we need and can afford.

Finally, we must not allow Congress or the Administration to overreact. This will be most difficult during election years. On some days, the hyperbole, hype and hollow promises of some politicians frighten me more than terrorists. Following the President's State of the Union address, a prominent Democratic leader stated that less than five percent of cargo entering the US is currently

inspected. She demanded that 100 percent of cargo that comes into this country by sea, and 100 percent of the cargo carried on domestic and international flights be inspected. That is a recipe for economic disaster. That is what I mean when I say the US government could do more damage to the American economy than terrorists.

It is important that I maintain my nonpartisan status, so let me go on the record that I have heard equally troubling statements from Republicans, such as spending billions of dollars securing our borders. According to the Department of Homeland Security, there are 7,000 miles of borders and 95,000 miles of shoreline in this country. Understanding that we are in this for the long-haul, how can we ever hope to seal our borders against terrorists? Imagine the costs. It is not economically feasible. We must *contain* our impulse for overreaction.

Spending Priorities

Mr. Chairman, it is from this perspective of *containment* that I offer my recommendations for spending priorities for Fiscal Year 2006 and beyond. The challenge will be to take these spending priorities and translate them into a national security system that was designed for a different threat and a different time.

To defend America from the Soviet threat, Congress provided funds to the Department of Defense and the intelligence community. For the threats of the 21st century, it will require funding programs in the Departments of Homeland Security, Health and Human Services, Justice, Agriculture, Defense, Treasury, the Environmental Protection Agency, the intelligence community, and state and local governments. One estimate stated that as many as 87,000 government jurisdictions are involved in homeland security--most, or perhaps all of which look to the US Congress for funding. How can you possibly establish priorities within all of these stovepipes?

My recommendation is that you focus your efforts on threats, not organizations. Some would tell you that the range of threats is nearly as diverse as the government organizations involved. That also may be true, but it is critical to understand that there are only two threats capable of bringing this nation to its knees--nuclear and biological weapons. These two threats must receive top priority for spending. Additionally, there is one other area that can provide the American taxpayer with the best return on investment for the broad range of threats we will face in the coming years--information technology. Information systems can provide substantial security benefits for the broad range of threats--from weapons of mass destruction to suicide bombers in shopping malls.

Nuclear Weapons

Since the United States lost its monopoly on nuclear weapons in 1949, no other weapon has emerged that equals severity of the nuclear threat. One Hiroshima-sized bomb in an American city would forever change the course of our history. A second nuclear weapon in a second city

would threaten the foundations of our political, economic, and social structures. A nuclear armed al Qaeda would be an existential threat to the United States of America. This is neither hyperbole nor fear mongering. It is simply a fact.

There are no means to mitigate the effects of a nuclear detonation. Once the Soviets improved the accuracy of their missiles, we learned that even a super-hardened facility such as Cheyenne Mountain was vulnerable. It is physically and economically impossible to harden America against a nuclear attack. Likewise, there is no effective response after an attack. Therefore, the only effective strategy is to prevent such an attack.

The good news in this case is that there is a relatively simple solution to preventing such an attack: do not let al Qaeda or another terrorist organization get their hands on weapons grade material. I am confident that no terrorist organization today, or at any time in the next decade will have the capability to enrich uranium to weapons grade levels or produce plutonium. The problem however, is that it only requires 35 pounds of highly-enriched uranium (HEU) or 9 pounds of plutonium to produce a bomb. In other words, a large briefcase could contain enough material to build a nuclear weapon.

Where would you find such material? It is not as difficult as you may think. There is enough HEU sitting in research reactors to build hundreds of Hiroshima-sized bombs. There are more than 100 such reactors, in 40 countries, that use HEU as their fuel. The fuel in these research reactors is generally not highly radioactive. Unlike the fuel rods in a nuclear power plant, these fuel elements would not require massive shielding to transport. Several research reactor fuel elements could be safely carried in an ordinary suitcase. A 1977 unclassified report from the Argonne National Laboratory stated that the processing required to convert these fuel elements into weapons grade material could be accomplished with commercial off-the-shelf equipment. Details on the chemical processes required is also available in open literature. (For more details on this issue see: Securing the Bomb: An Agenda for Action, Matthew Bubb & Anthony Wier, www.nti.org/cnwm)

In addition to the material in research reactors, there are hundreds of tons of weapons grade material inadequately protected in the former Soviet Union. Considerable money has been appropriated and some success has been achieved, but securing 99 percent of this material means that sufficient material would be available to terrorists to build scores of nuclear weapons. Additionally, we now have even more weapons-grade material to worry about, thanks to Dr. Khan in Pakistan.

Domestic Nuclear Detection Office

The newly created Domestic Nuclear Detection Office is certainly a worthwhile tactical effort, but not the strategic program we require. The two greatest shortfalls are clearly identified in the title of the new office: *domestic* and *detection*. While most details on the roles and responsibilities of this office have yet to be determined, the word *domestic* leads me to believe its focus will be inside US borders. Most of the nuclear material that we must contain is outside US borders. Additionally, *detecting* nuclear material inside our borders is the last

step in a long process, and what I would describe as a desperate effort with low probability of success.

America's goal must be to contain the proliferation of nuclear material and to prevent it from ever reaching our shores. That is where we should focus our spending. Nunn-Lugar type programs will provide America with the best return on investment for securing our homeland. **Without question, America's number one spending priority for FY 06 and beyond should be exactly what both Presidential candidates said at the end of their first televised debate on September 30, 2004--preventing the terrorists from getting their hands on weapons-grade nuclear materials.**

Biological Weapons

Protecting America against nuclear terrorism is a daunting challenge, but the action required is not complicated--we only need to prevent the terrorists from obtaining weapons-grade nuclear material. Unfortunately, protecting America against bioterrorism is far more complex and a far greater challenge. Equally troubling is the fact that the revolution in biotechnology means that the likelihood of a sophisticated biological attack during the next decade is far greater than a nuclear attack.

Going back to the strategy of *containment*, we must understand that it is impossible to prevent bioattacks. This was demonstrated a few years ago with a government program called Bacchus. A small team of scientists with no experience in the production of bioweapons or access to classified information on the process demonstrated how easy it is to make them using open sources and equipment bought over the Internet. They showed that the funding required to weaponize pathogens is less than the price of a luxury car. The seed stock for bioweapons--such as bacillus anthracis (anthrax), yersinia pestis (plague), and viral hemorrhagic fevers (Ebola and Marburg)--exist in laboratories around the globe. With the exception of variola virus (smallpox), all of the 40 pathogens tested in various bioweapons programs exist in nature.

The biological weapons genie is out the bottle. There is no legislation you can enact to prevent terrorist from obtaining and weaponizing these pathogens. It is only a matter of time until a significant bioterrorism event occurs. Therefore, the second priority for spending homeland security funds must be for the mitigation and response to a bioattack.

I have spent more than a decade studying the bioterror threat, and I must admit it is at times mind-boggling. I am fortunate to have worked with many of America's top experts in the field of biodefense. For specific details on the programs I recommend, I refer you to these experts. My comments are from the perspective of a national security strategist. From this perspective, I can tell you that a national public health system in the 21st century will be as important to national security as the Department of Defense was in the 20th century. And when I say public health, I also include the issue of food and water security. In fact, a bioattack on our food supply is one of the most likely scenarios.

Preparing America for the 21st century biothreat is far more complex than moving dollars around on a line-item budget. We must think strategically. The "all-hazards" approach that is endorsed by the Department of Homeland Security is a sound policy for most threats--man-made and natural. It does not, however, work for an attack with a contagious pathogen.

Organization

If one believes that a bioattack is likely at some point in the future, one must be appalled with how America is currently organized to defend itself. I often use the following analogy to describe this egregious situation.

"Many people have submitted plans to transform the Department of Defense for the 21st century. Here is my plan. Instead of having it centrally organized, I suggest that we do away with the Pentagon and give each county, one tank, one fighter plane, and one infantry platoon. Each state will be provided with a few Navy ships. There will be no standards for credentialing the officers or NCOs. Some will be political appointees. Funding will come from various sources, and money that is sent from Washington can be easily moved to other programs outside of defense."

Sound like a good idea? Well, that is a reasonable description of our current public health system in this country. In fact, it is not a system at all. In some states, like Maryland, the county public health offices all are under the centralized control of the state public health officer. In other states, such as New Jersey and Massachusetts, city and county public health offices are decentralized--marching to their own drummers. In South Carolina, there is no state official whose primary responsibility is public health. There are no nationally recognized standards for credentialing of state and local public health officers, and the funding of these offices comes from a hodgepodge of uncoordinated sources. Furthermore, it has not been uncommon for Federal bioterrorism funds to be to diverted to programs that have no connection to bioresponse efforts.

The bottom line is that America does not have a coordinated public health system. **I cannot in good faith recommend that you increase funding to state and local public health offices for biodefense until there is a national plan and a national system. Continuing to pour money into a non-functioning system will not improve our security.**

For more details on the state of our public health community see, *Drafted to Fight Terror: U.S. Public Health on the Front Lines of Biological Defense* by Dr. Elin A. Gursky, 2004. (http://www.homelandsecurity.org/bulletin/drafted_gursky.pdf)

I am not criticizing the half million people who work in state and local public health offices. Most are highly dedicated, overworked, and underappreciated. The problem is organization. As General Eisenhower said, "The right organization will not guarantee success but the wrong organization will guarantee failure." **Today, we are not properly organized to defend this nation against a biological attack. There is no biodefense leader or organization in America.** That should keep you awake at night.

Prior to the 1960s, environmental issues were primarily seen as state and local responsibilities. We have since learned that the only effective way to approach the issue is with a national strategy. The same is now true for biodefense. As was demonstrated in the Dark Winter exercise in June 2001, and most recently in the Atlantic Storm exercise in January 2005, contagious pathogens do not recognized borders--neither state nor national. (see: http://www.upmc-biosecurity.org/)

America requires a national system for biodefense. Someone must be in charge. This recommendation may not be well received from some state and local public health officers. They do not want Washington telling them what to do. I do not blame them; I understand their concerns. Much of what state and local public health offices do on a daily basis is unique to their locations. But during a crisis, we must have a national response capability.

Building such a national system will require the long-term commitment of significant funds, although it would likely be just a fraction of what is spent each year on National Missile Defense. I have never understood why we are spending more on defense against a delivery system than we do on defense against the actual weapons. A nuclear or biological weapon can be delivered in a variety of ways, and in my opinion, a missile is the least likely. If a nuclear or biological weapon were to be used against Washington DC, the most likely delivery system will be a small truck, a car, a briefcase, or the US Postal Service, as we witnessed in October 2001--not an intercontinental ballistic missile that would provide us with a return address.

Furthermore, some of the changes needed will not require enormous amounts of taxpayers' money. As one example, the State of Texas has more than 40,000 nurses who no longer work in health care. Creating a reserve corps of health care workers would required only a few weekends a year for training, but could deliver enormous surge capability during a crisis. It would provide the American taxpayer with a significant return on investment. The reserve component of the Department of Defense played a major role in winning the Cold War and it continues to play an important role today. Why not a homeland security reserve corps? **Not every solution requires a billion dollar price tag.**

Situational Awareness

One of my greatest frustrations is the lack of progress in developing and fielding a system to provide situational awareness during a bio crisis, either man-made or naturally occurring. While the technology exists to create such a system, one has not been deployed. America needs a system that would provide public health offices, medical staffs, and local, state and Federal officials with near real-time information on the spread of the disease and the resources available to respond. This one system would be a major step forward in our mitigation efforts. Without such a system, there is little or no hope of an adequate response.

Research & Development

When I mentioned bioweapons such as smallpox, anthrax, and plague, you need to understand that these are yesterday's weapons. The bioweapons that keep me awake at night are the pathogens we will face in the future. Unfortunately, this future could be 2005. A genetically engineered pathogen that is contagious, lethal and resistant to our vaccines and treatments would be an existential threat to America. It is a very real possibility, and it is why I say spending priorities must focus on the biological threat.

I am not an expert in the field of research and development programs for biodefense. However, I am a national security strategist, and I know that funding research and development for new vaccines and treatments is as important as funding new weapons systems for Department of Defense. Our technological prowess is our asymmetric advantage over the terrorists. It is an advantage we must exploit. For details, I recommend you seek advice from the University of Pittsburgh's Center for Biosecurity, headed by Dr. Tara O'Toole. The Center can provide you and your staff with detailed information on key biodefense research and development programs.

Agro-terrorism

Just prior to leaving office, the Secretary of Health and Human Services, Tommy Thompson said he was surprised that the terrorists had not yet attacked our food supply. I understand his concern. A biological attack on America's food supply is in many respects easier to conduct than a bioattack on people, as demonstrated in the Crimson Sky and Crimson Winter exercises. Just ask Senator Pat Roberts (R-KS). He played the role of the President in Crimson Sky, and had to order the killing of 50 million cloven hoofed animals to get the foot and mouth disease (FMD) epidemic under control.

Mr. Chairman, your state, Iowa, is the prime target for agro-terror, one of the most likely biothreats. The animal most susceptible to FMD is the hog. FMD will spread through a feedlot like a prairie fire through dry grassland. Iowa has 5.3 hogs for every human being--the most dense concentration of hogs in the US. FMD will not harm humans, but it would be an economic and environmental disaster for not only your state, but the entire nation. Just think, what would you do with 50 million carcasses?

Additional funding for laboratory facilities, an information network to link these labs and more training exercises are the best means to improve mitigation and response capabilities for agro-terrorism.

Goals & Dual-Benefits

The short-term goal for biodefense should be on information technology that will provide improvements in mitigation and response capabilities, primarily, in the area of situational awareness. The mid-term goal (FY 08-11) should be the creation of a national system that can detect, respond to, and mitigate catastrophic health crises, either man-made or naturally

occurring. The long-term goal should be focused on research and development programs that will best use our technological advantage to create revolutionary capabilities such as "bug to drug in 24 hours" (as recommended by the 2002 Defense Science Board study) and something called preclinical detection.

Preclinical detection can move the advantage from the attacker to the defender in both man-made and naturally occurring diseases. For instance, if everyone in this room were exposed to variola virus today during this hearing, we would not begin to show symptoms for at least seven days--some people would take as long as seventeen days to become ill. In other words, we would all be "walking time-bombs". Each of us would unknowingly be carrying a contagious and lethal disease. No currently available test could detect this disease in our bodies. Only when we became symptomatic, and began to experience high fever and rash, would today's laboratory tests diagnose smallpox. For us, it would be too late. There is no treatment available once the rash begins. Thirty percent of us would die, some would become blind, all would suffer extraordinary pain and carry the scars of smallpox pustules for life.

With preclinical detection, the variola virus could be detected soon after it entered our bodies. The smallpox vaccine is effective if given within four days of exposure. Likewise, early antibiotic treatment against anthrax and plague would make the difference between a bio-incident and a bio-catastrophe. Preclinical detection would not end the biothreat, but it would significantly *contain* the consequences. It could, over time, reduce the effects of such attacks to a degree that it would serve as a deterrent.

The ability to detect disease before the onset of symptoms should be one of your top funding priorities. This capability would also provide an incredible dual-benefit to the health of all Americans. For any disease, man-made or naturally occurring, early detection is critically important.

One great advantage of spending on biodefense is this dual-benefit. When you buy a new nuclear powered aircraft carrier for national security, you get a powerful weapons system to defend America against its enemies, but in the end, it is just a weapons system. **If you properly fund a biodefense system you will reduce the vulnerability of America to a bioattack or a naturally occurring epidemic, and at the same time, significantly improve health care and food security--an extraordinary return on investment for the American taxpayer.**

The US Congress has the power to reduce America's vulnerability to a bioattack. I hope and pray you do so before we experience a large attack, not after.

Information

Information is an area in which we have the asymmetric advantage over the terrorists. We must use it wisely, and in a manner consistent with the value we place on privacy and civil liberties. We must understand that **information is the weapon that terrorists fear most**. Much work has been accomplished by think tanks and other not-for-profits on how we can

use information technology without sacrificing our privacy. The Potomac Institute's work on the Project Guardian is one to be commended. They have designed a system that allows our incredible technology to outwit the enemy while at the same time involving all three branches of government to provide the oversight necessary to protect our privacy. (http://www.potomacinstitute.org/research/projectguardian/pgintro.htm)

Guarding our Ports with Information Systems

To best protect our ports, priority should be placed on information systems, not on more gates, guns, guards, and gamma detectors. In the Democratic response to the President's 2004 State of the Union message, there was a call to "inspect all of the containers that enter this country." It takes four hours to inspect a container, and even then there is a possibility weapons of mass destruction could go undetected. Moreover, it is too late once a nuclear weapon arrives at a US port. Ports themselves are primary terrorist targets. A nuclear detonation in one of our mega ports would have unimaginable economic and political consequences. Obviously, then, hands-on inspection of each of the six million containers that enter the country yearly is neither possible nor desired.

So what would be fiscally responsible and increase security? Inspect containers with information tools *before* they enter our ports. Today's information systems must be harnessed to track container contents all the way back to purchase orders. It can be accomplished in a manner that neither slows the pace of commerce nor burdens our transportation system with unreasonable costs. Such inspection systems and methodology would provide both deterrence and prevention.

So when you are faced with spending priorities on cargo security, focus on systems that reach beyond our borders, not within them. Focusing your spending programs on systems within the boundaries of our ports, would be the equivalent of putting radiation detectors outside of this building. When the nuke gets that close, it is too late.

Shortly after 9-11 many began talking of "pushing out our borders." This, however, is not best accomplished with a manpower intensive effort, but with an electronic border in cyber space. During the Cold War we called this competitive strategies. We must do the same today--funding those initiatives where we can best exploit our strengths against their weaknesses.

National Level Information Sharing

The sharing of information is another area that requires attention and funding support. The technologies exist today that would allow local, state and Federal law enforcement organizations, plus intelligence agencies, pass information to a common data hub for national level compilation and analysis. The hub will be the National Counter Terrorism Center, which also needs the capability to provide processed intelligence and information to local, state and Federal law enforcement agencies. Obviously, an oversight function is an essential element in a data-sharing system. (See Project Guardian at the Potomac Institute for the details on the oversight function.) Information technologies exist today that would have caught at least 11 of

the 19 hijackers before they boarded their airplanes on 9-11.The deployment of such a system should be one of your highest priorities.

Intelligence

Intelligence is a subset of information. Homeland security intelligence analysis requires the recruitment, training and employment of individuals with expertise in the high priority threat areas, such as nuclear and biological. The focus in the Department of Homeland Security information analysis office (as well as other intelligence agencies) has been current intelligence (the news cycle): what is hot today; what threat needs to be briefed to the Secretary; and what information is coming in from the Joint Terrorism Task Forces. The Department of Homeland Security objective has been to hire top-notch, recent graduates from America's universities who can function successfully in that current intelligence environment. We need those new analysts for the current intelligence mission, but to deal with the nuclear and biological threats we need intelligence analysts who understand the science as well as the political/international context.

Analysis is supposed to drive collection, not the other way around (a major contributor to our intelligence failures.) We need to build expertise on nuclear and biological threats in the information analysis office. This office should focus on the strategic threat, provide collection requirements to HUMINT, SIGINT and other collectors, and provide threat analysis to the Department of Homeland Security and other national security policymakers.

The Identity Question

There is one last area of information technology I must mention, one that is quite controversial: personal identification. Fifteen European nations already have a form of nationally standardized identification. The United Kingdom, after much debate, has recently decided to begin such a program.

Some would say that we already have one in the United States, our state-issued driver's license. We all use it every time we transit an airport. The only problem is, it does not provide us an effective anti-terrorism system. We have all heard the stories about the 9-11 hijackers--that seven had Virginia driver's licenses, and none lived in Virginia. There are some states with laws that authorize the issuance of driver's licenses to people who are known to be illegal aliens. We all know that any reasonably intelligent college student understands how to use the Internet to get a photo ID card that "proves" he or she is 21.

We are in the process of spending billions of dollars on the US-Visit program that was designed to deter or capture terrorists entering our country. If and when the system becomes highly effective, the terrorists will stop using our ports of entry and begin crossing our 7,000 miles of unguarded borders and 95,000 miles of shoreline. Remember, they are a thinking enemy. When we close and lock one door, they will move to another. We can spend ourselves into bankruptcy by staying just one step behind them.

Today, many Americans are not ready for a national identity system. I am one of them. However, if we experience several major attacks, larger and more deadly than 9-11, the American people may change their attitudes on this subject. A poll taken shortly after 9-11 stated that 70 percent of Americans favored a national identity system

I recommend that you give high priority to the study of this issue through the think-tank you created--the Homeland Security Institute. You should direct the Institute to lead the effort and examine four key issues:

1. Does an organization and system exist that can ensure identification credentials are properly issued?
2. Does the technology exist to create a means of identification that cannot be altered or counterfeited?
3. Can we build a system that is affordable?
4. Does the American public feel secure that such a system would protect their privacy?

Today, the answers are: no, yes, yes, no. The purpose of the study would be to determine if it is technologically and politically feasible to get four "yeses". Then, and only then, would I support such a system.

Perhaps, we should include a fifth question: Would such a system make us more secure? I believe the answer is yes. There is no way to effectively control 7,000 miles of borders and 95,000 miles of shoreline. If we spend billions making it virtually impossible for known terrorists to enter the United States through our sea, air and land ports, they will begin crossing our borders in the same way the economic refuges and migrant workers from Mexico and Central America have done for decades. And even though some members of Congress want to build impregnable borders with physical and electronic barriers, you must understand such an initiative would be no more effective protecting our homeland today than the Maginot Line was at protecting France in 1940. It would waste valuable resources and leave us no more secure.

One thing I know for sure--when I get on an airplane with my family, I would like to know that the person setting next to my daughter is not on a terrorist watch list. The system we have today does not provide me that security. After the next major attack, the question of identity will come up again. And when it does, it would be nice to think that our elected leaders had shown the strategic vision to look into the future, and to have some answers ready when the American public asks the question, "Why don't we have a nationally standardized identity system?'

Conclusion

America can survive a car bomb or two. America can survive an attack on a train, a shopping mall, chemical plant, or even another attack with an airplane. On the other hand, attacks with nuclear and biological weapons have the potential to radically change our political, social and economic foundations. They are in a class by themselves and must receive your top priority.

Unfortunately, America is not well organized for this challenge, particularly, the biological threat. Who is in charge of protecting America from biological attacks? There is no single person or single agency. The Departments of Homeland Security, Agriculture, Health and Human Services, Defense, the Environmental Protection Agency, the intelligence community, 50 states, 8 territories, and more than 3,000 counties are involved in the effort. We are spending billions without a national organization or effective plan. Not a recipe for success.

I know you have many pressures to provide homeland security funds for a wide variety of threats. I understand that every fire department, police department, sheriffs department, emergency management agency, and hospital in each of your home districts wants priority for homeland security funding. The demand is unlimited, but we must keep the other threats in perspective. Since 2001, no Americans have died in our homeland from terrorism. During the past three years: 15,000 have died from food poisoning, 120,000 have died from automobile accidents, nearly 300,000 have died from medical mistakes, 1,500,000 have died from cancer, and more than 2,000,000 have died from heart disease.

A nuclear weapon in an American city or an attack with a sophisticated biological weapon could exceed all of these numbers, combined. Either one of these attacks could easily exceed the number of Americans killed in all wars during the past 230 years.

Therefore, your priorities for homeland security funds must focus on preventing terrorists from obtaining weapons-grade nuclear material, building a national system to improve mitigation and response for bioattacks, and exploiting our asymmetric advantage in information systems. These are the priorities that will provide the American taxpayer with the best return on investment--a homeland that is secure from catastrophic attack and a nation that is making best use of its asymmetric advantage over the terrorists.

-end-